ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT



УДК 621.893 DOI 10.12737/12599

Исследование возможности применения генетических алгоритмов для реализации криптоанализа блочных криптосистем*

Ю. О. Чернышев[1], А. С. Сергеев[2], Н. Н. Венцов [3], А. Н. Рязанов[4]**
[1,2,3,4] Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Feasibility study of genetic algorithms application for implementation of block cryptosystem cryptanalysis ***

Y. O. Chernyshev [1], A. S. Sergeyev [2], N. N. Ventsov [3], A. N. Ryazanov [4]**
[1,2,3,4] Don State Technical University, Rostov-on-Don, Russian Federation

Рассматривается возможность применения алгоритмов генетического поиска для реализации криптоанализа блочных методов шифрования. Отличительной особенностью применения биоинспирированных методов криптоанализа (в частности, генетических методов) является возможность использования самого алгоритма шифрования (или расшифрования) в качестве целевой функции для оценки пригодности ключа, определенного с помощью генетических операций. Вследствие этого при использовании биоинспирированных методов криптоанализа процесс определения секретного ключа (например, при криптоанализе второго типа) зависит не столько от сложности шифрующих преобразований, сколько от самого биоинспирированного метода, который должен обеспечивать достаточное разнообразие генерации ключей, что свидетельствует об актуальности задачи исследования возможности применения биоинспирированных алгоритмов (в частности, методов генетического поиска) для криптоанализа блочных криптосистем. Отмечается также, что поскольку отличительной особенностью как блочных методов шифрования, так и генетических алгоритмов, является их внутренний параллелизм, то задача разработки алгоритма криптоанализа на основе параллельной реализации составляющих этапов является актуальной. Предлагается алгоритм криптоанализа блочных методов на примере стандарта DES на основе его параллельной версии, приводятся результаты эксперимента при определении квазиоптимального ключа, полученные при параллельной реализации алгоритма на 8-буквенных блоках текста. Отмечается, что временные затраты алгоритма не превосходят временных затрат при реализации известных методов криптоанализа.

Feasibility of genetic search algorithms application for implementation of the cryptanalysis of block cipher methods is considered. A distinctive feature of the bioinspired cryptanalysis methods application (in particular, genetic methods) is the possibility of using the encryption (or decryption) algorithm as an objective function for the suitability evaluation of the key defined by genetic operations. Consequently, when using the bioinspired cryptanalysis methods, the S key definition (for example, when using type 2 cryptanalysis) depends not so much on the complexity of the ciphering transformations, as on the bioinspired method which is to provide a sufficient variety of key generation that shows the significance of the research task of the bioinspired algorithms feasibility (in particular, genetic search methods) for the block cryptosystem cryptanalysis. It is noted also that as the distinctive feature of both block cipher methods, and the genetic algorithms is their internal parallelism, then the task of developing a cryptanalysis algorithm based on the parallel implementation of the constituent stages is relevant. An algorithm of the block methods cryptanalysis on the example of the DES standard on the basis of its parallel version is offered; the experiment results of the quasioptimal key determination obtained at the parallel algorithm implementation on the 8-letter text blocks are given. It is noted that time costs of the algorithm realization do not exceed the time of the known cryptanalysis implementation.

Ключевые слова: криптоанализ, генетический алгоритм, блочный алгоритм шифрования, популяция ключей, кроссинговер**,** квазиоптимальный ключ.

Keywords: cryptanalysis, genetic algorithm, block cipher algorithm, population of keys, crossover, quasioptimal key.

* Работа выполнена при финансовой поддержке РФФИ (проекты 13-01-00343, 14-01-00634, 15-05-00129).
** E-mail: myvnn@list.ru, sergeev00765@mail.ru, vencov@list.ru, alexandr_r89@mail.ru
*** The research is done with the financial support from RFBR (projects 13-01-00343, 14-01-00634, 15-05-00129).

Введение. В настоящее время при разработке компьютерных технологий, обеспечивающих информационную безопасность и защиту информации, широкое применение находят криптографические методы защиты. Для решения задач криптоанализа, относящихся к классу *NP*-полных, в последние годы применяются алгоритмы, основанные на природных системах. К ним относятся методы моделирования отжига, генетические алгоритмы (ГА), эволюционные методы, алгоритмы роевого интеллекта и т.д. В моделях и алгоритмах эволюционных вычислений ключевым элементом является построение начальной модели и правил, по которым она может изменяться (эволюционировать). В течение последних лет были предложены разнообразные схемы эволюционных вычислений, в т.ч. генетический алгоритм, генетическое программирование, эволюционные стратегии, эволюционное программирование.

В работе [1] рассматривались задачи криптоанализа и приведены результаты криптоанализа классических симметричных криптографических алгоритмов с использованием методов эволюционной оптимизации и генетического поиска для симметричных шифров перестановок, а также для реализации шифров простой и многоалфавитной замены. Среди обзорных работ, посвященных описанию методов и перспектив развития криптоанализа, следует отметить [2–4], в которых описаны универсальные методы (метод полного перебора, атака по ключам, частотный анализ, метод Полларда), методы криптоанализа симметричных (статистический метод, метод дифференциального анализа, метод линейного анализа) и асимметричных (задача дискретного логарифмирования, задача факторизации) криптосистем, а также новый вид криптоанализа — атаки по побочным каналам. В работе [2] также приводится краткое изложение новых технологий, связанных с использованием ГА, нейронных сетей и квантовых компьютеров.

Криптоанализ асимметричных алгоритмов шифрования описан в [4–6], где представлен ГА для решения задачи определения вариантов разложения заданного числа *N* на множители и ГА разложения заданного числа на два взаимно простых сомножителя, а также алгоритм нахождения простого делителя числа. В работе [7] представлены алгоритмы муравьиных и пчелиных колоний для разложения составных чисел на множители путем определения делителя числа с заданной точностью в заданном интервале. Описание алгоритма «пчелиных колоний» для реализации криптоанализа шифров перестановки, и сведение его к классической задаче о назначениях приведено в [8].

Метод криптоанализа блочного алгоритма. Таким образом, возникает вопрос о возможности применения биоинспирированных методов для криптоанализа современных блочных алгоритмов шифрования, т.к. переход к блочному шифрованию открывает дополнительные возможности для повышения стойкости криптоалгоритмов. Одним из приемов при шифровании является многократная, состоящая из нескольких циклов, обработка одного блока открытого текста. Основные принципы построения блочных шифров, структура алгоритмов блочного шифрования (схема Фейстеля) описаны, например, в [3].

Отличительной особенностью применения биоинспирированных методов криптоанализа (в частности, ГА) является возможность использования самого алгоритма шифрования (или расшифрования) в качестве целевой функции для оценки пригодности ключа, определенного с помощью генетических операций. Поэтому можно утверждать, что при использовании ГА процесс определения секретного ключа (например, при криптоанализе второго типа) зависит не столько от сложности шифрующих преобразований, сколько от самого биоинспирированного метода, который должен обеспечивать достаточное разнообразие генерации ключей. В этой связи задача исследования возможности применения биоинспирированных алгоритмов для криптоанализа блочных криптосистем является, несомненно, актуальной.

Рассмотрим организацию криптоанализа блочных методов с использованием ГА на примере представителя блочных шифров — стандарта DES.

Заметим, что важным свойством как блочных методов, так и ГА, является их внутренний параллелизм, основные модели параллельных ГА (глобальный параллельный ГА, островная модель, клеточный ГА) приведены в [1]. В этой связи для разработки криптоанализа данного алгоритма с помощью эволюционного подхода рассмотрим вначале процесс параллельной реализации составляющих его этапов. Исходя из непосредственного описания алгоритма, можно выделить следующие основные параллельно выполняемые этапы:

- параллельная обработка 64-битовых блоков шифртекста;
- параллельная обработка восьми 6-битовых блоков $B_1 \ldots B_8$;
- параллельная обработка блоков C_i и D_i и формирование ключей K_i.

С использованием этих очевидных преобразований схема одного цикла алгоритма представлена на рис. 1 [9].

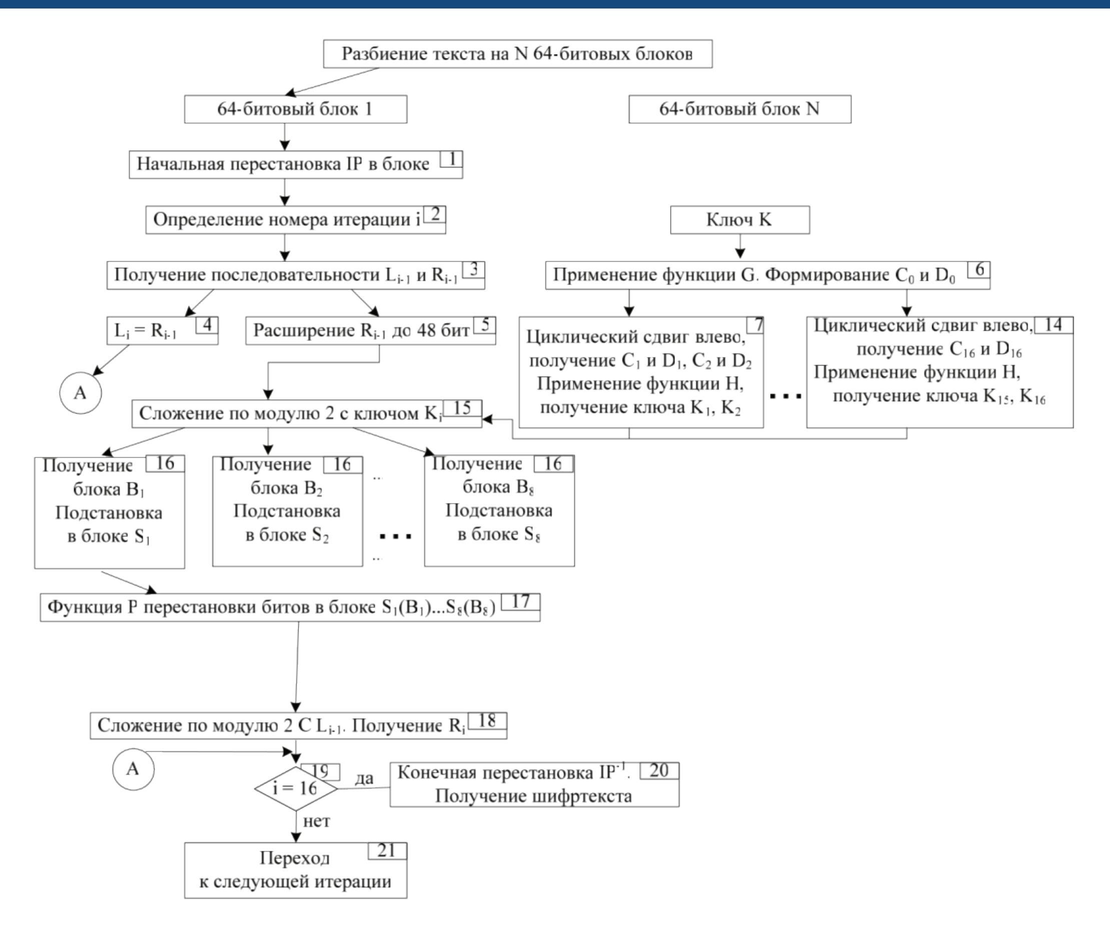


Рис. 1. Структурная схема цикла алгоритма DES

Для дальнейшего определения множества независимых операторов, допускающих параллельное выполнение, используются методы, описанные в [10, 11].

Построим информационно-логическую граф-схему $G = (X, U)$ алгоритма DES, где множество X вершин соответствует множеству операторов алгоритма, множество U дуг состоит из дуг, определяющих связи по управлению (двойная линия) и по информации (одинарная линия). Граф-схема алгоритма позволяет представить и проанализировать как общую структуру алгоритма, так и связи между отдельными операторами, и показана на рис. 2.

Для данного графа введем в рассмотрение матрицу следования S. Элемент $S(ij) = *$, если существует связь по управлению ($j \Rightarrow i$) и $S(ij) = 1$, если существует связь по информации ($j \rightarrow i$).

Используя алгоритм нахождения транзитивных связей, получим матрицу S_T [10, 11]. Далее введем в рассмотрение матрицу L логической несовместимости операторов, используя алгоритм, также приведенный в [10, 11]. Для объединения информации о логической несовместимости операторов и их информационно-логической связи откажемся от ориентированности графа G и построим матрицу S_T', полагая $(i, j) = (j, i) = 1$.

На матрицу S_T' наложим матрицу L, определив значение каждого элемента по правилам дизъюнкции. Получим матрицу независимости M, по нулевым элементам которой в строке (пробелам) можно указать множество тех операторов, каждый из которых может быть выполнен параллельно с оператором, соответствующим номеру строки. Структуры матриц S, S_T, L, S_T', M приведены в [9].

Таким образом, на основе построенной параллельной схемы алгоритма представим метод криптоаналитической атаки второго типа, т.е. при наличии известного текста и шифртекста требуется определить ключ K, используемый для шифрования, с целью дешифрования других сообщений, зашифрованных тем же ключом.

Поскольку секретность DES полностью определяется ключом, задачей эволюционного поиска является генерация популяции ключей и оценка их оптимальности с последующим применением стандартного набора генетических операций. То есть применение генетического поиска непосредственным образом для проведения криптоаналитической атаки второго типа при заданных 64-битовых блоках исходного текста и шифртекста можно представить структурной схемой, ГА показанной на рис. 3 (на схеме K_{ij}: i — номер индивидуума в популяции, j — номер варианта, используемого на j-й итерации).

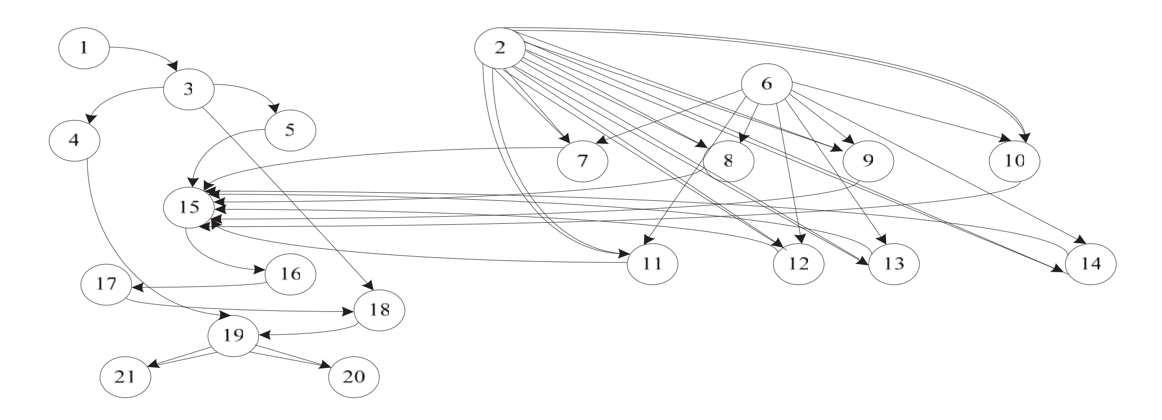


Рис. 2. Информационно-логическая граф-схема алгоритма *DES*

Как видно из схемы (рис. 3), после формирования начальной популяции ключей производится оценка их пригодности (определение целевой функции), т.е. проверка, насколько полученный с их помощью шифртекст совпадает с известным. После оценки производится селекция индивидуумов популяции для проведения множества генетических операций и получения множества потомков, далее полученная расширенная популяция подвергается дальнейшему оцениванию. Процесс заканчивается, когда прекращается эволюционирование популяции, либо когда исчерпан заданный временной ресурс (пройдено заданное количество генераций).

Следовательно, если сформирована популяция из P индивидуумов, то время работы алгоритма T составит $T = Pt$, где t — время оценки одного индивидуума (варианта ключа).

При значительном объеме популяции для определения функции пригодности индивидуумов можно использовать эффективный принцип организации специализированных вычислений — принцип конвейера [12]. Общая схема реализации потока операций на последовательном конвейере и описание процесса реализации представлены в [9].

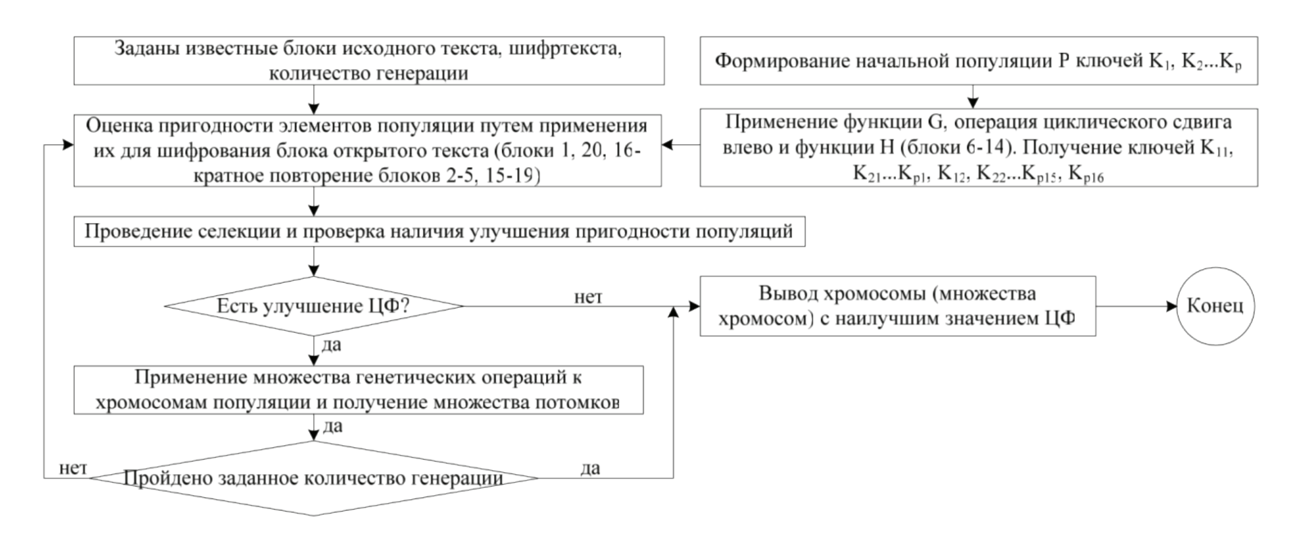


Рис. 3. Структурная схема генетического алгоритма

Таким образом, после разработки параллельной схемы реализации криптоанализа актуальной является задача: для алгоритма шифрования, используемого для оценки пригодности элементов популяции ключей, на основе построенного информационно-логического графа G и для заданного времени $T_{зад}$ найти необходимое наименьшее число процессоров однородной вычислительной системы и план выполнения операторов на них. Для решения этой задачи также использовались методы, изложенные в [10, 11], а ее решение представлено в [13]. При этом на основе визуальной методики [11] получена минимальная оценка числа процессоров n=2 при критическом пути в графе G $T_{кр}$=24, заданном времени $T_{зад}$=$T_{кр}$ и показано, что эта оценка является минимальной, а также определен план выполнения операторов.

На основе построенной параллельной схемы алгоритма разработан метод криптоаналитической атаки второго

типа. Алгоритм и его программная реализация включают следующие этапы:

1. Генерация популяции ключей по 64 бита (размер определяется экспериментально).
2. Оценка каждого элемента (ключа) популяции (блок CheckQuality).
3. Сортировка ключей по степени пригодности (блок QualitySolutionSort).
4. Проведение генетических операций (кроссинговер 80%, мутация и инверсия 0,05%).
5. Оценка расширенной популяции.
6. Сокращение популяции на 20% путем отсечения самых худших индивидуумов.
7. Возврат к 3.

Процесс заканчивается либо по истечении временного ресурса, либо по достижении оптимального или квазиоптимального варианта ключа.

Экспериментальные результаты. Приведем описание некоторых экспериментальных результатов, полученных при реализации ГА криптоанализа, проводимого с использованием процессора CORE I5-2400. Результаты для двух серий экспериментов представлены в таблицах 1, 2. При реализации эксперимента задавались следующие параметры: размер начальной популяции — 1000; количество итераций — 100; норма мутации и инверсии — 0,05; тип кроссинговера — простой двухточечный.

Таблица 1

Результаты сходимости ГА криптоанализа при 1 генерации

0	1000	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
1	1800	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
4	5372	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
5	7735	25,0	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
8	23094	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0
17	614816	37,5	37,5	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0
18	885334	37,5	37,5	37,5	37,5	37,5	37,5	37,5	25,0	25,0	25,0
20	1835828	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
22	3806771	50,0	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
23	5481748	50,0	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
25	11366950	50,0	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
30	23681145	62,5	50,0	50,0	50,0	50,0	50,0	37,5	37,5	37,5	37,5

В 1 столбце таблиц показан номер итерации, во 2 столбце — количество хромосом, подвергнувшихся мутации и инверсии, столбцы с 3 по 12 значение процента для 10 лучших хромосом популяции, определяющего совпадение полученного текста с исходным. Как видно из таблицы, на 25 генерации наилучшая хромосома обеспечивает совпадение полученного текста с исходным на 50%, на 30 генерации — на 62,5%.

Таблица 2

Результаты сходимости ГА криптоанализа при 2 генерации

0	1000	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
1	1800	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
4	5372	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
5	7735	25,0	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
8	23094	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0
15	294570	37,5	37,5	37,5	25,0	25,0	25,0	25,0	25,0	25,0	25,0
16	423775	50,0	37,5	37,5	37,5	37,5	25,0	25,0	25,0	25,0	25,0
17	614816	50,0	37,5	37,5	37,5	37,5	37,5	25,0	25,0	25,0	25,0
18	877847	50,0	37,5	37,5	37,5	37,5	37,5	25,0	25,0	25,0	25,0
20	1818165	50,0	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
21	2618158	50,0	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
25	11360920	50,0	50,0	50,0	37,5	37,5	37,5	37,5	37,5	37,5	37,5
30	23681145	62,5	62.5	50,0	50,0	50,0	50,0	37,5	37,5	37,5	37,5

Время реализации алгоритма для получения квазиоптимального ключа составило при одноточечном кроссинговере (мутации и инверсии 5%) 53 мин., при кроссинговере по маске 29 мин., при двухточечном кроссинговере 55 мин., что значительно меньше временных затрат при реализации дифференциального криптоанализа, приведенного в [14].

Приведем результаты эксперимента по определению квазиоптимального ключа, обеспечивающего максимальное совпадение полученного текста с исходным. В качестве исходного был использован следующий текст:
«я_вас_любил:_любовь_еще,_быть_может,_в_душе_моей_угасла_не_совсем;_но_пусть_она_вас_больше_не_тревожи
т;_я_не_хочу_печалить_вас_ничем.___»

При реализации алгоритма криптоанализа путем разбиения исходного текста на 8-буквенные блоки и использовании параллельного вычислительного процесса был определен квазиоптимальный ключ, обеспечивающий получение следующего текста:
«я*в*с*любил***юб*вь*еще**б*ть_*оже***в_д*ше*м*ей_**асла*не**овс*м*_н*_*ус*ь*о*а_в*с*бол**е_н*_т*ев*
ж*т;*я*н**хочу_п*ч*л*т*_ва*_**че*.__*»

Как можно заметить, полученный текст достаточно близок к исходному (совпадение в пределах 62,5%), содержит осмысленные слова (хочу, любил) или почти осмысленные (т*ев*ж*т, п*ч*л*т), из чего следует, что процесс расшифрования (например, при использовании ГА для криптоанализа первого типа) может быть доведен до конца вручную (аналогично тексту, полученного при использовании квазиоптимального ключа в ГА, описанном в [15]).

При втором эксперименте в качестве исходного был использован следующий текст:
«жил_старик_со_своею_старухой_у_самого_синего_моря;_они_жили_в_ветхой_землянке_ровно_тридцать_лет_и_три
_года._старик_ловил_неводом_рыбу,_старуха_пряла_свою_пряжу._раз_он_в_море_закинул_невод,_-
_пришел_невод_с_одною_тиной.____»

При реализации алгоритма криптоанализа и использовании параллельного вычислительного процесса был определен квазиоптимальный ключ, обеспечивающий получение следующего текста:
«жи*_с*а*и*_с*_сво*ю_*т*ру*ой_у_с**ог*_си*е*о_мо*я**о*и_**ли_в_в*тхо**з*мля*к*_р*вн**три**ат**лет*и_тр
и***да.*с*а*и*_лов*л*н*в*до*_рыб*,**та*уха**ряла*с**ю_*ряж*._р*з*о*_в*мор**зак***л_н*вод*_*_***шел_**во
д_с**дною*т*ной*__**»

Таким образом, при размере начальной популяции N=1000 был определен квазиоптимальный ключ, что свидетельствует о возможности экспериментального выбора параметров ГА. При экспериментальной реализации использовались простой одноточечный кроссинговер, кроссинговер по маске, двухточечный кроссинговер с нормой 80%, простая точковая мутация с нормой 5%. В процессе реализации ГА после формирования множества потомков и проведения генетических операций использовался элитный отбор для доведения размера популяции до исходного состояния. В случае, если при реализации алгоритма криптоанализа был определен квазиоптимальный ключ, обеспечивающий совпадение полученного текста с исходным на 62,5% и более, результат криптоанализа считался достигнутым.

Заключение. Описано применение ГА для реализации криптоанализа блочных криптосистем, приведены результаты эксперимента при реализации криптоанализа второго типа алгоритма DES на основе параллельной схемы его реализации. Временные затраты алгоритма не превосходят временных затрат при реализации известных методов криптоанализа. Как показали результаты эксперимента, полученные результаты по определению оптимального ключа (при криптоанализе второго типа) в общем случае в значительной степени зависят от длины исходного текста, что может привести к эффективному использованию вычислительных систем, допускающих параллельную обработку информации (в частности, многопроцессорных систем класса SIMD).

Библиографический список

1. Чернышев, Ю. О. Криптографические методы и генетические алгоритмы решения задач криптоанализа / Ю. О. Чернышев, А. С. Сергеев, Е. О. Дубров, О. П. Третьяков. — Краснодар : ФВАС, 2013. — 138 с.

2. Авдошин, С. М. Криптоанализ : современное состояние и перспективы развития / С. М. Авдошин, А. А. Савельева // Информационные технологии. — 2007. — № 3. — С. 1–32.

3. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л. К. Бабенко, Е. А. Ищукова. — Москва : Гелиос АРВ, 2006. — 376 с.

4. Чернышев, Ю. О. Обзор алгоритмов решения задач криптоанализа на основе биоинспирированных технологий искусственного интеллекта / Ю. О. Чернышев, А. С. Сергеев, Е. О. Дубров // Вестник Воронеж. гос. ун-та. — 2014. — № 2. — С. 83–89.

5. Сергеев, А. С. О возможности применения методов генетического поиска для реализации криптоанализа асимметричного алгоритма шифрования данных *RSA* / А. С. Сергеев // Известия ВУЗов. Сев.-Кавк. регион. Технические науки. — 2008. — № 3. — С. 48–52.

6. Чернышев, Ю. О. Применение биоинспирированных алгоритмов оптимизации для реализации криптоанализа классических и асимметричных криптосистем / Ю. О. Чернышев, А. С. Сергеев, Е. О. Дубров // Информатика : проблемы, методология, технологии : материалы XIV междунар. науч.-метод. конф. — Воронеж, 2014.

— С. 206–210.

7. Сергеев, А. С. Биоинспирированные методы криптоанализа асимметричных алгоритмов шифрования на основе факторизации составных чисел / А. С. Сергеев, О. П. Третьяков, А. Е. Васильев, Ю. О. Чернышев // Вестник Дон. гос. техн. ун-та. — 2011. — Т. 11, № 9(60). — С. 1544–1554.

8. Чернышев, Ю. О. Исследование возможности применения бионических методов пчелиных колоний для реализации криптоанализа классических шифров перестановок / Ю. О. Чернышев, А. С. Сергеев, Е. О. Дубров, А.Н. Рязанов // Вестник Дон. гос. техн. ун-та. — 2014. — Т. 14, № 1(76). — С. 62–75.

9. Сергеев, А. С. Исследование и разработка методов генетического поиска для организации криптоанализа блочных криптосистем в системах управления безопасностью и защиты информации на примере стандарта шифрования *DES* / А. С. Сергеев // Третья междунар. конф. по проблемам управления : пленарные доклады и избранные труды. — Москва, 2006. — С. 328–335.

10. Барский, А. Б. Планирование параллельных вычислительных процессов / А. Б. Барский. — Москва : Машиностроение, 1980. — 191 с.

11. Сергеев, А. С. Параллельное программирование / А. С. Сергеев. — Ростов-на-Дону : Издательский центр ДГТУ, 2002. — 77 с.

12. Воеводин, В. В. Математические модели и методы в параллельных процессах / В. В. Воеводин. — Москва : Наука, 1986. — 296 с.

13. Сергеев, А. С. Разработка генетического метода криптоанализа блочных криптосистем и исследование возможности их параллельной реализации в системах защиты информации на примере стандарта *DES* / А. С. Сергеев // Системный анализ в проектировании и управлении : тр. 10 междунар. науч.-практ. конф. — Санкт-Петербург, 2006. — С. 258–265.

14. Бабенко, Л. К. Применение параллельных вычислений при решении задач защиты информации / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидоров // Программные системы : теория и приложения. — 2013. — № 3(17). — С. 25–42.

15. Морозенко, В. В. Генетический алгоритм для криптоанализа шифра Вижинера / В. В. Морозенко, Г. О. Елисеев // Вестник Пермск. гос. ун-та. Серия : Математика. Механика. Информатика. — 2010. — № 1. — С. 75–80.

References

1. Chernyshev, Y.O., Sergeyev, A.S., Dubrov, E.O., Tretyakov, O.P. Kriptograficheskie metody i geneticheskie algoritmy resheniya zadach kriptoanaliza. [Cryptographic methods and genetic algorithms for solving cryptanalysis problems.] Krasnodar: FVAS, 201, 138 p. (in Russian).

2. Avdoshin, S.M., Savelieva, A.A. Kriptoanaliz: sovremennoe sostoyanie i perspektivy razvitiya. [Cryptanalysis: Current State and Future Trends.] Information Technologies, 2007, no. 3, pp. 1–32 (in Russian).

3. Babenko, L.K., Ishchukova, E.A. Sovremennye algoritmy blochnogo shifrovaniya i metody ikh analiza. [Modern block encryption algorithms and methods of their analysis.] Moscow: Gelios ARV, 2006, 376 p. (in Russian).

4. Chernyshev, Y.O., Sergeev, A.S., Dubrov, E.O. Obzor algoritmov resheniya zadach kriptoanaliza na osnove bioinspirirovannykh tekhnologiy iskusstvennogo intellekta. [Review of the algorithms cryptanalysis on the basis bioinspired methods of artificial intelligence.] Proceedings of Voronezh State University, 2014, no. 2, pp. 83–89 (in Russian).

5. Sergeyev, A.S. O vozmozhnosti primeneniya metodov geneticheskogo poiska dlya realizatsii kriptoanaliza asimmetrichnogo algoritma shifrovaniya dannykh RSA. [On applicability of genetic search methods for the implementation of asymmetric data RSA encryption algorithm cryptanalysis.] Izvestiya vuzov. Severo-Kavkazskiy region. Technical Sciences. 2008, no. 3, pp. 48–52 (in Russian).

6. Chernyshev, Y.O., Sergeyev, A.S., Dubrov, E.O. Primenenie bioinspirirovannykh algoritmov optimizatsii dlya realizatsii kriptoanaliza klassicheskikh i asimmetrichnykh kriptosistem. [Application of bioinspired optimization algorithms for the implementation of classic and asymmetric cryptosystem cryptanalysis.] Informatika: problemy, metodologiya, tekhnologii: materialy XIV mezhdunar. nauch.-metod. konf. [Computer science: problems, methodology, technologies: Proc. XIV Int. Sci.-Method. Conf.] Voronezh, 201, pp. 206–210 (in Russian).

7. Sergeyev, A.S., Chernyshev, Y.O. Bioinspirirovannye metody kriptoanaliza asimmetrichnykh algoritmov shifrovaniya na osnove faktorizatsii sostavnykh chisel. [Cryptanalysis bioinspired methods of asymmetric key on the basis of composite number factorization.] Vestnik of DSTU, 2011, vol. 11, no. 9(60), pp. 1544–1554 (in Russian).

8. Chernyshev, Y.O., Sergeyev, A.S., Dubrov, E.O., Ryazanov, A.N. Issledovanie vozmozhnosti primeneniya bionicheskikh metodov pchelinykh koloniy dlya realizatsii kriptoanaliza klassicheskikh shifrov perestanovok. [Research on applicability of bionic techniques of artificial bee colonies for implementation of classical transposition cipher cryptanalysis.]

Vestnik of DSTU, 2014, vol. 14, no. 1(76), pp. 62–75 (in Russian).

9. Sergeyev, A.S. Issledovanie i razrabotka metodov geneticheskogo poiska dlya organizatsii kriptoanaliza blochnykh kriptosistem v sistemakh upravleniya bezopasnost'yu i zashchity informatsii na primere standarta shifrovaniya DES. [Research and development of genetic search methods for the organization of block cryptosystem cryptanalysis in the safety management systems and data protection using an example of the standard DES encryption.] Tret'ya mezhdunar. konf. po problemam upravleniya : plenarnye doklady i izbrannye trudy. [III Int. Conf. on control problems: plenary paperss and selecta.] Moscow, 2006, pp. 328–335 (in Russian).

10. Barskiy, A.B. Planirovanie parallel'nykh vychislitel'nykh protsessov. [Planning of parallel computing processes.] Moscow: Mashinostroenie, 198, 191 p. (in Russian).

11. Sergeyev, A.S. Parallel'noe programmirovanie. [Parallel programming.] Rostov-on-Don: DSTU Publ. Centre, 2002, 77 p. (in Russian).

12. Voyevodin, V.V. Matematicheskie modeli i metody v parallel'nykh protsessakh. [Mathematical models and methods in parallel processes.] Moscow: Nauka, 1986, 296 p. (in Russian).

13. Sergeyev, A.S. Razrabotka geneticheskogo metoda kriptoanaliza blochnykh kriptosistem i issledovanie vozmozhnosti ikh parallel'noy realizatsii v sistemakh zashchity informatsii na primere standarta DES. [Development of the genetic method of block cryptosystem cryptanalysis and feasibility study of their parallel implementation in information security systems on the example of DES standard.] Sistemnyy analiz v proektirovanii i upravlenii: tr. 10 mezhdunar. nauch.-prakt. konf. [System analysis in the design and management: Proc. X Int.-Pract. Conf.] St. Petersburg, 2006, pp. 258–265 (in Russian).

14. Babenko, L.K. Ishchukova, E.A., Sidorov, I.D. Primenenie parallel'nykh vychisleniy pri reshenii zadach zashchity informatsii. [Application of parallel calculations at the solution of information protection problems.] Program Systems: Theory and Applications, 2013, no. 3(17), pp. 25–42 (in Russian).

15. Morozenko, V.V., Eliseev, G.O. Geneticheskiy algoritm dlya kriptoanaliza shifra Vizhinera. [A genetic algorithm for cryptoanalysis of Vigener’s cipher.]Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2010, no. 1, pp. 75–80 (in Russian).

Поступила в редакцию 08.04.2015
Сдана в редакцию 08.04.2015
Запланирована в номер 30.06.2015